FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Canadian Centre for Cyber Security

May 2023

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: TIMOTHY HALL Digitally signed by TIMOTHY HALL Date: 2023.06.02 17:05:20 -04'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: King, Lyall Digitally signed by King, Lyall DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall" Reason: I am approving this document Location: Date: 2023.06.02 14:06:08-04'00' Foxit PDF Editor Version: 12.1.2

Dated: _____

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4496	05/01/2023	CBL-Mariner OpenSSL Cryptographic Module	Microsoft Corporation	Software Version: 2.0
4497	05/02/2023	FortiGate Next-Generation Firewalls with FortiOS 6.4/7.0	Fortinet, Inc.	Hardware Version: FortiGate-40F (C1AJ53) [1] [2], FortiGateRugged-60F (C1AJ89) [1] [2], FortiGate-60F (C1AJ22) [1] [2], FortiGate-61F (C1AJ23) [1] [2], FortiWiFi-60F (C1AJ24) [1] [2], FortiWiFi-61F (C1AJ25) [1] [2], FortiGate-80F (C1AK17) [1] [2], FortiGate-81F (C1AK18) [1] [2], FortiGate-100F (C1AJ43) [1] [2], FortiGate-101F (C1AJ44) [1] [2], FortiGate-200F (C1AJ87) [1] [2], FortiGate-201F (C1AJ88) [1] [2], FortiGate-600E (C1AH98) [1] [2], FortiGate-601E (C1AH71) [1] [2], FortiGate-1100E (C1AJ67) [1] [2], FortiGate-1101E (C1AJ13) [1] [2], FortiGate-1800F (C1AJ82) [1], FortiGate-1801F (C1AJ83) [1], FortiGate-2600F (C1AK55) [1], FortiGate-2601F (C1AK56) [1], FortiGate-3300E (C1AJ42) [1] [2], FortiGate-3301E (C1AJ38) [1] [2], FortiGate-3400E (C1AH84) [1] [2], FortiGate-3401E (C1AH85) [1] [2], FortiGate-3600E (C1AH86) [1] [2], FortiGate-3601E (C1AH57) [1] [2], FortiGate-4200F (C1AH81) [1], FortiGate-4201F (C1AJ94) [1], FortiGate-4400F (C1AH79) [1], FortiGate-4401F (C1AJ45) [1], FortiGate-6300F (C1AG83) [1], FortiGate-6301F (C1AG85) [1], FortiGate-6500F (C1AG84) [1] and FortiGate-6501F (C1AG86) [1] with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.4 (FIPS-CC-64-5) [1] and FortiOS 7.0 (FIPS-CC-70-6) [2]
4498	05/02/2023	Red Hat Enterprise Linux 7 NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel7.20190606
4499	05/02/2023	Encryption Card ADVA 9TCE-PCN-10GU+AES10G-F	ADVA Optical Networking SE	Hardware Version: HW B-1.01; shelves: SH9HU (Version HW 2.01, Part Number 1078700121 F7/SH9HU), SH7HU (Version HW 2.05, Part Number 0078700101 F7/SH7HU), SH7HU-R (Version HW 2.05, Part Number 0078700111 F7/SH7HU-R), SH1HU-R/PF (Version HW 1.01, Part Number 1078700060-01 F7/SH1HU-R/PF), SH1HU-HP/2DC (Version HW 2.11, Part Number 1078700144 F7/SH1HU-HP/2DC), SH1HU-HP/E-TEMP/2DC (Version HW 1.01, Part Number 1078700145-01 F7/SH1HU-HP/E-TEMP/2DC); labels and label kits: SEAL/FIPS-GENERAL (Part Number 1013700030-01), SEAL/FIPS-WIRE (Part Number 1013700032-01), SEAL/FIPS-GENERAL/5 (Part Number BC00000738); Firmware Version: 172.25.7, 191.4.8

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4500	05/02/2023	Encryption Card ADVA 10TCE-PCN-16GU+AES100G-F	ADVA Optical Networking SE	Hardware Version: HW B-1.01; shelves: SH9HU (Version HW 2.01, Part Number 1078700121 F7/SH9HU), SH1HU-R/PF (Version HW 1.01, Part Number 1078700060-01 F7/SH1HU-R/PF), SH1HU-HP/2DC (Version HW 2.11, Part Number 1078700144 F7/SH1HU-HP/2DC), SH1HU-HP/E-TEMP/2DC (Version HW 1.01, Part Number 1078700145-01 F7/SH1HU-HP/E-TEMP/2DC); labels and label kits: SEAL/FIPS-GENERAL (Part Number 1013700030-01), SEAL/FIPS-CFP (Part Number 1013700031-01), SEAL/FIPS-WIRE (Part Number 1013700032-01), SEAL/FIPS-GENERAL/5 (Part Number BC00000738); Firmware Version: 172.21.1, 191.4.1
4501	05/02/2023	Maximus Federal Cryptographic Module	Maximus Federal	Software Version: 2.2.1
4502	05/03/2023	PTX10008 and PTX10016 Packet Transport Routers with Routing Engine JNP10K-RE0 and MACsec Line Card LC1105-M	Juniper Networks, Inc.	Hardware Version: PTX10008 and PTX10016 with components identified in Security Policy Table 1; Firmware Version: Junos OS 20.3X75
4503	05/03/2023	Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers with RE-S-X6-128G/RE-1800 Routing Engine and MPC7E-10G MACSec Card	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960 with components identified in Security Policy Table 1; Firmware Version: Junos OS 20.3X75
4504	05/03/2023	Juniper Networks PTX1000 Packet Transport Router	Juniper Networks, Inc.	Hardware Version: PTX1000; Firmware Version: Junos OS 20.3X75
4505	05/03/2023	Cryptographic Module for BIG-IP (R)	F5, Inc.	Software Version: 14.1.0.3 [1] and 14.1.2 [2]
4506	05/03/2023	Oracle OpenSSL FIPS Provider	Oracle Corporation	Software Version: 3.0.0
4507	05/04/2023	Acme Packet VME	Oracle Communications	Software Version: S-Cz9.0
4508	05/05/2023	SUSE Linux Enterprise Server Kernel Crypto API Cryptographic Module	SUSE, LLC	Software Version: 3.0
4509	05/05/2023	Juniper OpenSSL Cryptographic Module	Juniper Networks, Inc.	Software Version: 1.0
4510	05/05/2023	StarSign PIV Applet V 1.0 on Giesecke+Devrient Sm@rtCafé Expert 7.0	Giesecke+Devrient Mobile Security GmbH	Hardware Version: SLE78CLFX4000P (M7892); Firmware Version: Sm@rtCafé Expert 7.0, StarSign PIV Applet V1.0
4511	05/05/2023	Code Integrity	Microsoft Corporation	Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3]
4512	05/05/2023	Secure Kernel Code Integrity	Microsoft Corporation	Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3]

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4513	05/08/2023	SonicWall Capture Security Appliance (CSa) 1000	SonicWall	Hardware Version: 101-500644-50 Rev A; Firmware Version: 1.2
4514	05/08/2023	MPU5	Persistent Systems, LLC	Hardware Version: P/N WR-5100, Versions: 4.0.B, 4.1.B, 4.2.B, 4.2.C, 4.3.A, 4.3.B, 4.3.C, 4.3.D, 4.4.B, 4.4.C, 4.4.D, 4.5.C, 4.5.D, 4.6.D, 4.6.K, 4.6.L, 4.6.L.1, 4.6.M, 4.6.N, 4.9.N, 4.9.O and 4.9.P; Tamper Evident Paint P/N PROD-007; Firmware Version: 19.6.10
4515	05/08/2023	Kernel Mode Cryptographic Primitives Library	Microsoft Corporation	Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3]
4516	05/08/2023	Cisco ASR 9000 Aggregated Services Routers	Cisco Systems, Inc.	Hardware Version: [ASR-9006-SYS with components A9K-RSP5-TR, A9K-RSP880-TR, A9K-16X100GE-TR], [ASR-9010-SYS with components A9K-RSP5-TR, A9K-RSP880-TR, A9K-16X100GE-TR], ASR-9901, [ASR-9904 with components A9K-RSP5-TR, A9K-RSP880-TR, A9K-16X100GE-TR, A99-8X100GE-TR, A99-12X100GE, A99-32X100GE-TR], [ASR-9906 with components A9K-RSP5-TR, A9K-16X100GE-TR, A99-8X100GE-TR, A99-12X100GE, A99-32X100GE-TR], [ASR-9910 with components A9K-RSP5-TR, A9K-16X100GE-TR, A99-8X100GE-TR, A99-12X100GE, A99-32X100GE-TR], [ASR-9912 with components A99-RP3-TR, A9K-16X100GE-TR, A99-8X100GE-TR, A99-12X100GE, A99-32X100GE-TR] and [ASR-9922 with components A99-RP3-TR, A9K-16X100GE-TR, A99-8X100GE-TR, A99-12X100GE, A99-32X100GE-TR]; Firmware Version: IOS-XR 7.1.2
4517	05/09/2023	IDPrime 3930 FIDO	Thales	Hardware Version: SLE78CLFX400VPH (A1714221) and SLE78CLFX400VPH (A1633310); Firmware Version: IDCore3130 - Build 12G, IDPrime 3930 Applet V4.5.0F, MSPNP Applet V1.2, FIDO V2.0.4B Applet
4518	05/10/2023	Secure Boot Processor (SBP) Crypto Engine	Fungible, Inc.	Hardware Version: F1 1.0.0 and S1 1.0.1; Firmware Version: 95b53165a1
4519	05/11/2023	Cisco Catalyst 9400 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst 9404R, Cisco Catalyst C9407R and Cisco Catalyst C9410R with components C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-48U, C9400-LC-48T, C9400-LC-48P, C9400-LC-24XS, C9400-LC-48UX, C9400-LC-24S, C9400-LC-48S and C9400-LC-48H; Firmware Version: Cisco IOS-XE 16.12 and Cisco IOS-XE 17.3
4520	05/11/2023	Cisco Catalyst 9600 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst 9606R with components C9600-SUP-1, C9600-LC-48YL and C9600-LC-24C; Firmware Version: Cisco IOS-XE 16.12 and Cisco IOS-XE 17.3
4521	05/16/2023	Look-aside Cryptography and Compression Engine (LCE)	Google, LLC	Hardware Version: 3.0; Firmware Version: B1.4.1 FW 6023
4522	05/17/2023	Inseego 5G Cryptographic Module	Inseego Corp.	Software Version: 2.2.1

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4523	05/19/2023	AWS Key Management Service HSM	Amazon Web Services, Inc.	Hardware Version: 3.0; Firmware Version: 1.7.100, 1.7.102 and 1.7.103
4524	05/24/2023	Uplogix LM80, LM83X, 500, and 5000	Lantronix, Inc.	Hardware Version: 80-8S-NNN-YAA, 83X-8S-000-YAA, 61-5050-33 and 61-5500-33 with 61-0001-00; Firmware Version: 6.1.1.39602g
4525	05/26/2023	Cisco Catalyst 9500 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst C9500-32C, Cisco Catalyst C9500-32QC, Cisco Catalyst C9500-48YC, Cisco Catalyst C9500-24YC, Cisco Catalyst C9500-24Q, Cisco Catalyst C9500-12Q, Cisco Catalyst C9500-40X and Cisco Catalyst C9500-16X with components C9500-NM-8X and C9500-NM-2Q; Firmware Version: Cisco IOS-XE 16.9.2, Cisco IOS-XE 16.12 and Cisco IOS-XE 17.3
4526	05/31/2023	Embedded Module and Embedded Module Lite	Persistent Systems, LLC	Hardware Version: P/Ns WR-5200, Versions 4.0, 6.0, 7.0, 7.A, 8.A and 12.B and WR-5250, Versions 1.0, 3.0, 3.A and 12.B; Firmware Version: 19.6.10
4527	05/31/2023	Embedded Module and Embedded Module Lite	Persistent Systems, LLC	Hardware Version: P/Ns WR-5200, Versions 4.0, 6.0, 7.0, 7.A, 8.A and 12.B and WR-5250, Versions 1.0, 3.0, 3.A and 12.B; Firmware Version: 19.6.10